

Original document**INITIALIZATION METHOD AND UBS DRIVER**

Publication number: JP2004094514

Publication date: 2004-03-25

Inventor: NUNOURA TAKEFUMI; YAMAMOTO HIROSHI; SUZUKI  
MASANORI; MORIMOTO MASASHI; SHIOBARA TETSUYA

Applicant: JAPAN RADIO CO LTD

Classification:

- international: **G06F13/14; G06F13/38; G06F13/14; G06F13/38; (IPC1-7): G06F13/14; G06F13/38**

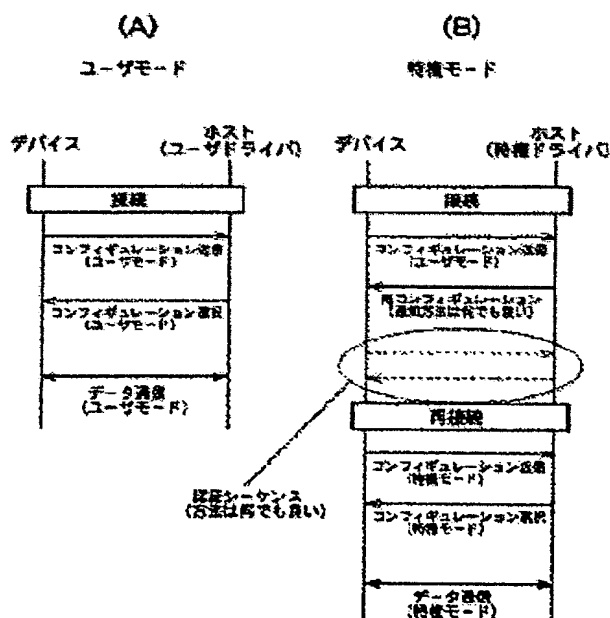
- European:

Application number: JP20020253754 20020830

Priority number(s): JP20020253754 20020830

[View INPADOC patent family](#)[View list of citing documents](#)[Report a data error here](#)**Abstract of JP2004094514****PROBLEM TO BE SOLVED:** To prevent a privilege mode from being inferred by a general user.**SOLUTION:** Configuration data for the general user are transmitted in a device side to conduct data communication by a user mode when a configuration thereof is selected (A). When the configuration thereof is not selected, a configuration data for a privilege user is transmitted after an authentication procedure or the like to conduct data communication by a privileged mode when a configuration thereof is selected (B). A host concerned in the general user selects the configuration data for the general user (A), and a host concerned in the privileged user requires reconfiguration to try reconnection by the configuration data for the privileged user (B).

COPYRIGHT: (C)2004,JPO

Data supplied from the *esp@cenet* database - Worldwide

**JP2004094514:** No description available

---

Data supplied from the *esp@cenet* database - Worldwide

**JP2004094514:** No claims available

---

Data supplied from the *esp@cenet* database - Worldwide

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-94514

(P2004-94514A)

(43) 公開日 平成16年3月25日(2004. 3. 25)

(51) Int. Cl.<sup>7</sup>

G06F 13/14

G06F 13/38

F I

G06F 13/14 330A

G06F 13/38 350

テーマコード(参考)

5B014

5B077

審査請求 有 請求項の数 6 O L (全 13 頁)

(21) 出願番号	特願2002-253754 (P2002-253754)	(71) 出願人	000004330
(22) 出願日	平成14年8月30日(2002. 8. 30)		日本無線株式会社
			東京都三鷹市下連雀5丁目1番1号
		(74) 代理人	100075258
			弁理士 吉田 研二
		(74) 代理人	100096976
			弁理士 石田 純
		(72) 発明者	布浦 武文
			東京都三鷹市下連雀5丁目1番1号 日本無線株式会社内
		(72) 発明者	山本 弘
			東京都三鷹市下連雀5丁目1番1号 日本無線株式会社内

最終頁に続く

(54) 【発明の名称】 初期化方法及びUSBドライバ

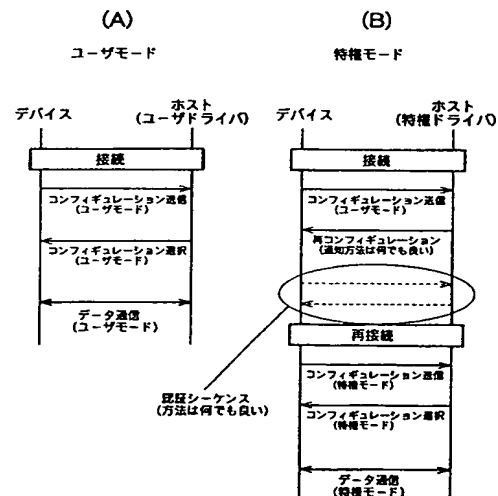
## (57) 【要約】

【課題】特権モードが一般ユーザに察知されないようにする。

【解決手段】デバイス側では、一般ユーザ向けのコンフィギュレーションデータを送信して、そのコンフィギュレーションが選択されたらユーザモードでのデータ通信を行う(A)。逆に、そのコンフィギュレーションが選択されなかった場合は、認証手順等を経た上で、特権ユーザ向けのコンフィギュレーションデータを送信して、そのコンフィギュレーションが選択されたら特権モードでのデータ通信を行う(B)。一般ユーザに係るホストが、一般ユーザ向けのコンフィギュレーションデータを選択するのに対し(A)、特権ユーザに係るホストは、再コンフィギュレーションを要求して、特権ユーザ向けのコンフィギュレーションデータによる再接続を試行する(B)。

【選択図】

図3



## 【特許請求の範囲】

## 【請求項1】

USBデバイスの機能構成を示すコンフィギュレーションデータをUSBデバイスからUSBホストへと送信するステップ及びこの送信への応答としてUSBホストからUSBデバイスにUSB通信開始許可又は拒否を通知するステップを含む初期化手順を、USBデバイスをUSBホストに接続する際にUSBデバイス・USBホスト間通信により実行する初期化方法において、USBホストからUSB通信開始拒否が通知されたときに、先に送信したコンフィギュレーションデータにより特定される機能構成とは別の機能構成を示す他のコンフィギュレーションデータをUSBデバイスから送信することによって、初期化手順を再実行させることを特徴とする初期化方法。

10

## 【請求項2】

請求項1記載の初期化方法において、初期化手順の再実行を、USBホストからUSBデバイスへとUSB通信開始許可が通知されるまで、また使用するコンフィギュレーションデータを逐次変更しつつ、所定回数を限度として繰り返すことを特徴とする初期化方法。

## 【請求項3】

請求項1又は2記載の初期化方法において、初期化手順を再実行する際に、コンフィギュレーションデータの送信に先立ち、USBデバイス・USBホスト間通信により、USBデバイスがUSBホストを認証するため又はUSBデバイス・USBホスト間の相互認証のための認証手順を実行することを特徴とする初期化方法。

20

## 【請求項4】

請求項1乃至3のいずれか一項記載の初期化方法において、最初に実行される初期化手順にて送受信されるコンフィギュレーションデータが、一般ユーザ向けのコンフィギュレーションデータであり、再実行に係る初期化手順にて送受信されるコンフィギュレーションデータが、一般ユーザとは異なる権限を有する特権ユーザ向けのコンフィギュレーションデータであることを特徴とする初期化方法。

## 【請求項5】

請求項4記載の初期化方法を実行するためUSBデバイスにインストールされるデバイス側USBドライバにおいて、上記USBデバイスがUSBホストに接続されたときに、そのUSBホストに対し上記USBデバイスの機能構成を示しかつ一般ユーザ向けのコンフィギュレーションデータを送信し、それに対する応答としてUSB通信開始許可が通知された場合に、接続先のUSBホストとのデータ通信を開始させ、接続先のUSBホストからUSB通信開始拒否が通知された場合に、接続先のUSBホストが特権ユーザに係るホストであるとし、そのUSBホストに対し特権ユーザ向けのコンフィギュレーションデータを送信して、USB通信開始許可を求めることを特徴とするデバイス側USBドライバ。

30

## 【請求項6】

請求項5記載のデバイス側USBドライバがインストールされたUSBデバイスが接続されるUSBホストに、請求項4記載の初期化方法を実行するため、インストールされるホスト側USBドライバにおいて、新たに接続されたUSBデバイスからそのUSBデバイスの機能構成を示すコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては一般ユーザ向けのコンフィギュレーションデータであるとし、送信元のUSBデバイスに対しUSB通信開始拒否を通知し、通知先のUSBデバイスから前回とは異なるコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては特権ユーザ向けのコンフィギュレーションデータであるとし、USB通信開始許可及び拒否のいずれかを通知することを

40

50

特徴とするホスト側USBドライバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、USB(Universal Serial Bus)デバイスをUSBホストに接続したときに実行される初期化方法、並びにこの初期化方法の実施に適するUSBドライバに関する。

【0002】

【従来の技術】

USBデバイス(以下単に「デバイス」)をUSBホスト(以下単に「ホスト」)例えばPCに接続する際には、デバイス・ホスト間通信により初期化(エニュメレーション)手順が実行される。初期化手順においては、デバイスの機能構成即ちコンフィギュレーションを示すコンフィギュレーションデータが、デバイスからホストへと送信される(コンフィギュレーション送信)。その際、複数通りのコンフィギュレーションデータをデバイスからホストへと送信することもできる。ホストは、受信したコンフィギュレーションデータの中から、そのデータにより特定されるコンフィギュレーション下でのデータ通信を許可できるものを選択して、その結果をデバイスに通知する(コンフィギュレーション選択)。これらのステップを含む初期化手順を経た上で、デバイス・ホスト間で、USBインタフェースによるデータ通信が開始される。なお、受信したコンフィギュレーションデータにより特定されるコンフィギュレーション(群)のなかに、データ通信開始を許可できるコンフィギュレーションが見あたらない場合、ホストはデータ通信を拒否する。

【0003】

また、複数通りのコンフィギュレーションをとりうるデバイスをホストに接続する際には、例えば、上述の通り、各コンフィギュレーションに対応する合計複数通りのコンフィギュレーションデータがデバイスからホストに送信される。目的・用途によっては、複数通りのコンフィギュレーションデータのうちの1つにより初期化手順が実行され、その結果に応じて他のコンフィギュレーションデータにより初期化手順が実行されることもある。例えば、下記特許文献1に記載のデバイスでは、デバイスからホストへのソフトウェア類(ドライバ、ユーティリティ等)の転送に適する第1のコンフィギュレーションと、通常の方法でデータ転送に適する第2のコンフィギュレーションとが、準備されている。デバイスをホストに接続すると、第1のコンフィギュレーションを示すコンフィギュレーションデータがホストに送られ、このコンフィギュレーションデータ中に含まれている識別情報等に従ってホストがデバイスからドライバ等を受信及びインストールする。その後、第2のコンフィギュレーションを示すコンフィギュレーションデータがホストに送られ、適宜、データ通信が開始される。従って、デバイスをホストに接続するだけで、そのデバイス用のドライバ、ユーティリティ等の更新版をホストに自動インストールできる。

【特許文献1】

特開2000-194645号公報

【0004】

【発明が解決しようとする課題】

デバイスに複数通りのコンフィギュレーションを設ける目的としては、上掲のインストール自動化の他に、ユーザ種別によるコンフィギュレーションの切替等がある。ここでいうユーザ種別とは、そのデバイスをその本来用途通りに使用する一般ユーザ、一般ユーザとは異なる権限を有する特権ユーザ等の区別のことである。USBポートを有する通信端末を例とすると、USBポートを有するPC等にその通信端末をUSB接続して通信を行うユーザが、一般ユーザに該当する。これに対して、その通信端末の保守、点検等のサービスを行う者のように、一般ユーザとは異なる目的及び権限でその通信端末を使用する者が、特権ユーザに該当する。一般ユーザと特権ユーザの権限は、例えば、デバイス内に格納されている情報、特に秘密保持義務が課されている情報に対するアクセス権等において、相違している。具体的には、漏洩することを防ぐべき個人情報等に対しては、特権ユーザ

10

20

30

40

50

はアクセスできても一般ユーザはアクセスできないようにすべきである。

【0005】

こういった目的を達成するための一手法として、一般ユーザ向けのコンフィギュレーションと特権ユーザ向けのコンフィギュレーションを個々別々に準備する、という手法がある。その場合、図12に示すように、デバイスをホストに接続した直後に、一般ユーザ向けのコンフィギュレーションデータ及び特権ユーザ向けのコンフィギュレーションデータを、デバイスからホストに送信する。これら2通りのコンフィギュレーションデータを受信したホスト、具体的にはそのホストで使用しているUSBドライバ（以下単に「ドライバ」）は、それらのうち一方を選択する。例えば、一般ユーザ向け即ち通常のデータ通信のドライバであるユーザドライバはインストールされているが、特権ユーザ向け即ち保守等の特殊用途向けのドライバである特権ドライバはインストールされていない、というホストにおいては、図12（A）に示すように、一般ユーザ向けのコンフィギュレーションが選択され、そのコンフィギュレーション下でのデータ通信即ちユーザモードでのデータ通信が実行される。これに対して、特権ドライバがインストールされているUSBホストにおいては、図12（B）に示すように、特権ユーザ向けのコンフィギュレーションが選択され、そのコンフィギュレーション下でのデータ通信即ち特権モードでのデータ通信が実行される。

【0006】

このようにすれば、一般ユーザと特権ユーザの別に依りて、デバイスのコンフィギュレーションを切り替えてデータ通信を行うことができる。しかしながら、図12に示した手法では、USBの規格・仕様に倣い、一般ユーザ向け及び特権ユーザ向けの合計2通りのコンフィギュレーションデータを同時一括送信し、ホスト側でコンフィギュレーション選択を行っている。これは、初期化シーケンスを実行し始める時点ではホストのユーザが一般か特権かをデバイスで認識できていないためであり、従来型の手順の単純応用では余儀なくされる措置であるけれども、反面、一般ユーザが使用しているホストが特権モードの存在を知ってしまうという問題を生じさせる。特権モードの存在が知られるということは、例えば、デバイス内に格納されておりユーザモードではアクセスできない情報にアクセスするための迂路の存在が、一般ユーザに知られる、ということである。技術力と意欲又は遊戯心を持ったユーザならば、この迂路を通じて個人情報を入力することや、特権モード用のコンフィギュレーションデータと上掲の迂路を通じて入手した情報に基づき特権ドライバを自前で作成すること等が、可能である。一般ユーザ向け及び特権ユーザ向けの合計2通りのコンフィギュレーションデータを同時一括送信することには、このような情報セキュリティ面での問題を含め、いくつかの問題がある。

【0007】

本発明の目的の一つは、初期化シーケンスを特権ユーザ以外に特権モードの存在が察知されにくい手順にすること、またそれに適するドライバを提供することにある。

【0008】

【課題を解決するための手段】

このような目的を達成するために、本発明は、（1）デバイスの機能構成を示すコンフィギュレーションデータをデバイスからホストへと送信するステップ及びこの送信への応答としてホストからデバイスにUSB通信開始許可又は拒否を通知するステップを含む初期化手順を、デバイスをホストに接続する際にデバイス・ホスト間通信により実行する初期化方法において、（2）ホストからUSB通信開始拒否が通知されたときに、先に送信したコンフィギュレーションデータにより特定される機能構成とは別の機能構成を示す他のコンフィギュレーションデータをデバイスから送信することによって、初期化手順を再実行させることを特徴とする。より好ましくは、（3）初期化手順の再実行を、ホストからデバイスへとUSB通信開始許可が通知されるまで、また使用するコンフィギュレーションデータを逐次変更しつつ、所定回数を限度として繰り返すこととする。更に好ましくは、（4）初期化手順を再実行する際に、コンフィギュレーションデータの送信に先立ち、デバイス・ホスト間通信により、デバイスがホストを認証するため又はデバイス・ホスト

間の相互認証のための認証手順を実行することとする。また、例えば、(5)最初に実行される初期化手順にて送受信されるコンフィギュレーションデータは、一般ユーザ向けのコンフィギュレーションデータであり、(6)再実行に係る初期化手順にて送受信されるコンフィギュレーションデータは、一般ユーザとは異なる権限を有する特権ユーザ向けのコンフィギュレーションデータであるものとする。

【0009】

また、本発明は、(7)上掲の認証機能を備え一般ユーザ向け及び特権ユーザ向けにそれぞれコンフィギュレーションデータが準備されたデバイスにインストールされるデバイス側ドライバにおいて、(8)上記デバイスがホストに接続されたときに、そのホストに対し上記デバイスの機能構成を示しかつ一般ユーザ向けのコンフィギュレーションデータを送信し、それに対する応答としてUSB通信開始許可が通知された場合に、接続先のホストとのデータ通信を開始させ、(9)接続先のホストからUSB通信開始拒否が通知された場合に、接続先のホストが特権ユーザに係るホストであると見なし、そのホストに対し特権ユーザ向けのコンフィギュレーションデータを送信して、USB通信開始許可を求めることを特徴とする。本発明は、(10)上掲のデバイス側ドライバがインストールされたデバイスが接続されるホストにインストールされるホスト側ドライバにおいて、(11)新たに接続されたデバイスからそのデバイスの機能構成を示すコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては一般ユーザ向けのコンフィギュレーションデータであるの見なし、送信元のデバイスに対しUSB通信開始拒否を通知し、(12)通知先のデバイスから前回とは異なるコンフィギュレーションデータを受信した場合に、そのコンフィギュレーションデータに関しては特権ユーザ向けのコンフィギュレーションデータであるの見なし、USB通信開始許可及び拒否のいずれかを通知することを中心とする。

【0010】

【発明の実施の形態】

以下、本発明の好適な実施形態に関し図面に基づき説明する。

【0011】

図1及び図2に本発明の実施環境の一例を示す。これらの図のうち、図1に示したのはハードウェア構成、図2に示したのはソフトウェア構成である。本発明は、これらの図に示されているように、PHS端末等のデバイス10と、PC等のホスト20とを、USBケーブルにて接続したシステム環境にて実施可能である。

【0012】

また、デバイス10は、MPU11、RAM12、ROM13、クロック発生部14、USBコントローラ15等のハードウェアを有している。アプリケーションプログラム100やドライバ101等のソフトウェア類や、これらのソフトウェアにより使用されるデータ例えばコンフィギュレーションデータは、例えばROM13に予め書き込んでおく。MPU11は、RAM12によって提供される記憶空間を利用してこれらのソフトウェアに従い処理を実行し、デバイス10全体の動作を制御・管理する。クロック発生部14は、デバイス10の動作速度を規定するクロックを発生させる。USBコントローラ15は、USB接続のためのハードウェアである。

【0013】

アプリケーションプログラム100は、ドライバ101を介してUSBを使用する。ドライバ101は、API(Application Programming Interface)102、通信制御103、プロトコル制御104、認証処理105等のモジュールにより構成されている。API102は、アプリケーションプログラム100やその実行環境であるOS等とのインタフェースである。通信制御103は、USBコントローラ15による通信動作を制御する。プロトコル制御104は、USBのプロトコルに則って通信動作を管理・制御する。認証処理105は、プロトコル制御104の一部であり、後述の認証手順を担う。

【0014】

10

20

30

40

50

ホスト 20 のハードウェア構成については、PC を初めとする情報処理装置の分野において常識的な構成であるため、特に説明しない。また、ホスト 20 においても、アプリケーションプログラム 200 がドライバ 201 を通じて USB を使用する、というソフトウェア構成が採られている。このドライバ 201 のモジュール構成は、ドライバ 101 のそれと同様である。但し、ドライバ 201 を構成する各モジュールの必須機能は、ドライバ 101 を構成する各モジュールの必須機能と、異なっている。この相違は、一つには、デバイス 10 向けとホスト 20 向けというインストール先の相違による相違や、インストール先の OS 等の相違による相違であり、いわゆる当業者であれば本願による開示から容易に推察できる。また、ドライバ 101 とドライバ 201 における対応モジュール間の機能上の相違は、また一つには、後述の諸機能を実現するための相違である。この相違については、いわゆる当業者であれば、本願による開示から、一意に理解できるであろう。

#### 【0015】

図 3 に、本実施形態における初期化手順を示す。この初期化手順は、デバイス 10 が USB ケーブルによりホスト 20 に接続され、デバイス 10 とホスト 20 とが USB ケーブルにより接続されたことが周知の手法により検出された直後に、ドライバ 101 とドライバ 201 との通信により実行される手順であり、本発明に係る初期化方法の好適な実施形態の一つである。この手順は、より詳細には、主としてプロトコル制御 104 及びその一部である認証処理 105、並びにこれらに対応するドライバ 201 の構成モジュールにより、実行される。また、先にも述べたとおり、USB における通常の初期化手順は、デバイス 10 のコンフィギュレーションを示すコンフィギュレーションデータをデバイス 10 からホスト 20 に送信し、ホスト 20 では受信したコンフィギュレーションデータの採否判断・選択を行い、その結果をデバイス 10 に通知する処理を含んでいる。本実施形態における初期化手順でも、同様の処理を実行する。しかしながら、本実施形態における初期化手順は、図 12 に示した初期化手順とは異なり、一般ユーザ向け即ちユーザモード用のコンフィギュレーションを示すコンフィギュレーションデータと特権ユーザ向け即ち特権モード用のコンフィギュレーションを示すコンフィギュレーションデータとを一括送信する、という処理を含んでいない。

#### 【0016】

即ち、本実施形態では、まずユーザモードに係るコンフィギュレーションデータが、デバイス 10（厳密にはそのドライバ 101、以下同様）からホスト 20（厳密にはそのドライバ 201、以下同様）へと送信される。ホスト 20 が一般ユーザに係るホストである場合は、そのホスト 20 は、このユーザモード用のコンフィギュレーションデータについてコンフィギュレーション選択を実行し、その結果をデバイス 10 に通知する。USB 通信開始許可を表す通知であれば、図 3（A）に示すように、USB インタフェースによるデータ通信が開始される。ユーザモード用のコンフィギュレーションデータに基づく接続であることから、このデータ通信は、ユーザモードに係るコンフィギュレーションでの通信となる。この流れにおいては、特権モードに係るコンフィギュレーションデータは送信されないため、一般ユーザに係るホスト 20 が初期化手順の実行を通じて特権モードの存在を知ることはない。

#### 【0017】

逆に、ホスト 20 が特権ユーザに係るホストである場合は、そのホスト 20 は、受信したコンフィギュレーションの内容如何によらず、図 3（B）に示すように、デバイス 10 に対して再コンフィギュレーションを要求する。再コンフィギュレーションの要求は、例えばベンダーコマンドへの割当のように USB 規格に合致する方法の他、実用上差し障りがない場合は特権モード要求（図 5 参照）等のコマンドを追加するという USB 規格外の方法によっても、実行できる。再コンフィギュレーションの要求を受けたデバイス 10 は、ホスト 20 を相手として、デバイス 10・ホスト 20 間の相互認証手順（或いは少なくともデバイス 10 がホスト 20 を認証する手順）を実行する。認証一致という結果が得られた場合に限り、デバイス 10 は、USB コントローラ 15 に内蔵されるフルアンプ抵抗を電氣的にターンオンさせること等によって、ホスト 20 側に、デバイス 10 がホスト 20



から一旦切り離され再度接続されたかのように、認識させる。デバイス10は、その上で、特権モードに係るコンフィギュレーションデータをホスト20に送信し、ホスト20は、これに応じ、コンフィギュレーション選択を実行し、更にその結果に応じて、デバイス10・ホスト20間のデータ通信が開始される。特権モード用のコンフィギュレーションデータに基づく接続であることから、このデータ通信は、特権モードに係るコンフィギュレーションでの通信となる。

#### 【0018】

また、図3に示した手順では、ユーザモード及び特権モードという2種類のモードを想定していた。即ち、特権ユーザを全てひとくくりにしていた。これに対して、特権ユーザをレベル分けし、デバイス10・ホスト20間でやりとりできる情報の種別に関する制限の度合いを特権モードレベル毎に設定し、特権モードレベル毎にコンフィギュレーションを設定することも可能である。

#### 【0019】

仮に、特権ユーザのレベル即ち特権モードレベルが、低い方から順にレベル1、レベル2、レベルNの各レベルに分かれており（N：2以上の自然数）、接続先のホスト20がレベルIの特権ユーザに係るホストであるとする（I：1以上N以下の自然数）。この場合、例えば図4（A）に示すように、ホスト20が、再コンフィギュレーション要求に係るコマンド中に自分の特権モードレベルIを示す情報をセットしてそのコマンドを送信する。デバイス20は、認証一致と判断された後に、レベルIの特権ユーザ向けのコンフィギュレーションを示すコンフィギュレーションデータを送信することによって、初期化手順を開始・再実行する。この手順では、ホスト20の特権モードレベルが、認証前にデバイス10側に知られる。

#### 【0020】

これに対して、図4（B）に示すように、特権モードレベルの昇順に従い、特権モードコンフィギュレーション送信／再コンフィギュレーション要求を繰り返す、という手順では、平均的に見れば図4（A）よりも時間がかかるけれども、認証前にホスト20の特権モードレベルがデバイス10側に漏れることはなくなる。即ち、図4（B）に示した手順では、デバイス10が、レベル1、レベル2、という順で、最大でレベルNまで、そのレベルに係る特権ユーザ向けのコンフィギュレーションを示すコンフィギュレーションデータを、送信する。ホスト20では、自分の特権モードレベルに合致したコンフィギュレーションデータを受信した場合はそのコンフィギュレーションを選択し、そうでない場合は再コンフィギュレーションを要求する。ホスト20がコンフィギュレーションを選択する旨をデバイス10に通知した後、データ通信が開始される。

#### 【0021】

また、図4（A）又は（B）に示した手順における再コンフィギュレーション要求を、特権モード要求等のUSB規格外コマンドに置き換えた図5（A）又は（B）の手順によって、本発明を実施することもできる。図5（A）に示した手順では、ホスト20が特権モード要求に係るコマンド中に自分の特権モードレベルをセットして送信し、デバイス10では認証一致後にこの特権モードレベルに対応したコンフィギュレーションデータによる初期化手順を開始・再実行する。図5（B）に示した手順では、ホスト20が特権モード要求に係るコマンド中に自分の特権モードレベルをセットせずに送信し、デバイス10では認証一致後に特権モードレベルの昇順に従いレベルNまでを限度として各特権モードレベルに対応したコンフィギュレーションデータによる初期化手順を繰り返して実行する。

#### 【0022】

なお、図3～図5に示したいずれの手順においても、デバイス10からホスト20に特権モードレベルに関する通知を要求する等の動作は、実行されない。これは、一般ユーザに係るホスト20に特権モードの存在を知られることを、防ぐためである。

#### 【0023】

認証手順は、例えば図6（A）或いは（B）に示した手順により実行できる。図6（A）に示したパターンによる認証手順では、デバイス10からホスト20への認証要求及びホ

10

20

30

40

50

スト 20 からデバイス 10 への認証応答に、それぞれデバイス 10 又はホスト 20 の認証コードが含まれており、それらの認証コードに基づきデバイス 10、ホスト 20 又はその双方にて、双方の認証コード間に認証論理上の がないかどうかの判断即ち認証一致判断を行う（ホスト 20 のみで一致判断を行う場合はその結果をホスト 20 からデバイス 10 に通知する）。図 6（B）に示したパターンによる認証手順では、ホスト 20 からの再コンフィギュレーション要求に係るコマンド中に、ホスト 20 の認証コードが含まれている。また、図 6（A）における認証要求及び認証応答に代えて、それぞれ、デバイス 10 の認証コードを含む認証応答と、ホスト 20 における認証一致判断の結果を示す認証応答通知とが、送信される。いずれのパターンによるにしろ、認証一致であれば、前述の通り特権モードでの再接続のため特権モードに係るコンフィギュレーションデータにより初期化手順が実行され、認証不一致であれば、ホスト 20 からの再コンフィギュレーション要求が正当なものでない等の可能性があるため、特権モードに係るコンフィギュレーションデータによる初期化手順は実行されない（切断状態となる）。なお、認証手順を別途並列的に実行することも可能である。

#### 【0024】

図 7～図 11 に、図 3 及び図 6（A）に示した手順を例として、ドライバ 101 及び 201 の動作の流れを示す。図 7 及び図 8 はドライバ 101 の、図 9 は一般ユーザに係るホスト 20 のドライバ 201 の、図 10 及び図 11 は特権ユーザに係るホスト 20 のドライバ 201 の、動作の流れである。デバイス 10 がホスト 20 に接続されそのことが認識されると（300、400）、ドライバ 101 によりユーザモード用のコンフィギュレーションデータが送信され（301）、そのデータがドライバ 201 により受信される（401）。ホスト 20 が一般ユーザに係るホストである場合は、そのホスト 20 のドライバ 201 によるコンフィギュレーション選択（402）の結果に応じて（302、303）、デバイス 10・ホスト 20 間のデータ通信が開始される（304、403）。逆に、ホスト 20 が特権ユーザに係るホストである場合は、そのホスト 20 のドライバ 201 による再コンフィギュレーション要求（404）に応じて（302、303）、ドライバ 101 からの認証要求（305、405）及びドライバ 201 からの認証応答（406、306）を含む認証手順が実行され、ドライバ 101 側で認証一致判断を行う。このときドライバ 201 側では「切断」と認識しているため（407）、ドライバ 101 側で認証不一致と判断された場合はそのまま「切断」状態が続く（408）。これに対して、ドライバ 101 側で認証一致と判断されると、ドライバ 101 ではフルアップ抵抗ターンオン等により「再接続」状態に移行し（309）、ドライバ 201 はこれを以て「新規接続」と認識する（409）。その後、ドライバ 101 は特権モードに係るコンフィギュレーションデータを送信し（310、410）、ドライバ 201 はコンフィギュレーション選択を実行し（411、311）、しかる後、適宜、特権モードでのデータ通信が行われる（312、412）。

#### 【0025】

なお、以上の説明では、一般ユーザと特権ユーザとを想定していたが、本発明は、このような前提を必要とするものではない。即ち、本発明は、例えばハードウェア上の制約でコンフィギュレーションをいちどきに 1 種類しか送信できないデバイスから、ホストに対し複数通りのコンフィギュレーションを送信する手順としても、実施できる。

#### 【0026】

##### 【発明の効果】

このように、本発明によれば、あるコンフィギュレーションについてホストから USB 通信開始拒否との通知を受けたデバイスが、先のコンフィギュレーションとは別のコンフィギュレーションにより初期化手順を再実行するようにしたため、特権ユーザ以外に特権モードの存在が察知されにくい形で特権モードを設けることや、ハードウェア等の制約でコンフィギュレーション送信が制限されているデバイスからの複数通りのコンフィギュレーション送信が、可能になる。例えば、まず一般ユーザ向けのコンフィギュレーションデータにより初期化手順を実行し、通信開始が拒否されたときは特権ユーザ向けのコンフィギ

ュレーションデータにより初期化手順を実行する、という手順によって、一般ユーザに係るホストに特権モードの存在を知られること、ひいては不必要な情報流出等の問題を防止・解消できる。また、特に特権モードでの接続に当たって、デバイスがホストを認証するため又はデバイス・ホスト間の相互認証のための認証手順を実行することにより、上掲の問題は更に少なくなる。また、本発明は、一般にN通り（N：2以上の自然数）のコンフィギュレーションを想定して実施すること、例えばN階層の特権モードレベルを各特権ユーザに付与して各特権モードレベル毎に異なるコンフィギュレーションによる接続とすることができ、そのための手順として、ホストからの特権モードレベル通知を含む手順だけでなく、デバイス側で最大N回に亘り初期化手順の再実行を繰り返す手順も採用できる。そして、本発明によれば、上掲の効果を、ドライバの改良によって達成できる。

10

【図面の簡単な説明】

【図1】本発明のハードウェア的实施環境例を示す図である。

【図2】本発明のソフトウェア的实施環境例を示す図である。

【図3】本発明の第1の実施形態における初期化手順を示す図であり、特に（A）はホストが一般ユーザに係るホストであった場合を、（B）はホストが特権ユーザに係るホストであった場合を、それぞれ示すシーケンス図である。

【図4】本発明の他の実施形態に係る初期化手順を示す図であり、特に（A）は第2の実施形態を、（B）は第3の実施形態を、それぞれ示すシーケンス図である。

【図5】本発明の他の実施形態に係る初期化手順を示す図であり、特に（A）は第4の実施形態を、（B）は第5の実施形態を、それぞれ示すシーケンス図である。

20

【図6】本発明の好適な実施形態における認証手順の例を示す図であり、特に（A）は認証要求／認証応答による手順を、（B）は再コンフィギュレーション／認証応答／認証応答通知による手順を、それぞれ示すシーケンス図である。

【図7】本発明の第1の実施形態におけるデバイス側のドライバの動作の流れのうち前半を示すフローチャートである。

【図8】本発明の第1の実施形態におけるデバイス側のドライバの動作の流れのうち後半を示すフローチャートである。

【図9】本発明の第1の実施形態におけるホスト側のドライバの動作の流れ、特に一般ユーザに係るホストにおける流れを示すフローチャートである。

【図10】本発明の第1の実施形態におけるホスト側のドライバの動作の流れ、特に特権ユーザに係るホストにおける流れの前半を示すフローチャートである。

30

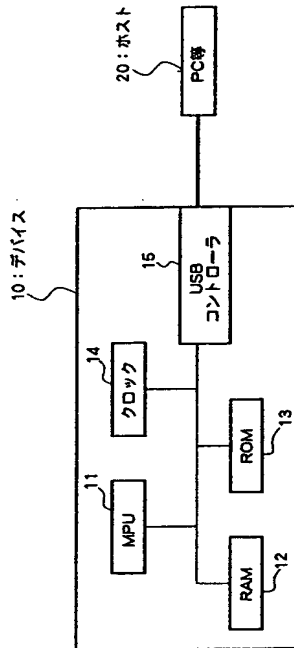
【図11】本発明の第1の実施形態におけるホスト側のドライバの動作の流れ、特に特権ユーザに係るホストにおける流れの後半を示すフローチャートである。

【図12】従来技術の単純変形による初期化手順を示す図であり、特に（A）はホストが一般ユーザに係るホストであった場合を、（B）はホストが特権ユーザに係るホストであった場合を、それぞれ示す図である。

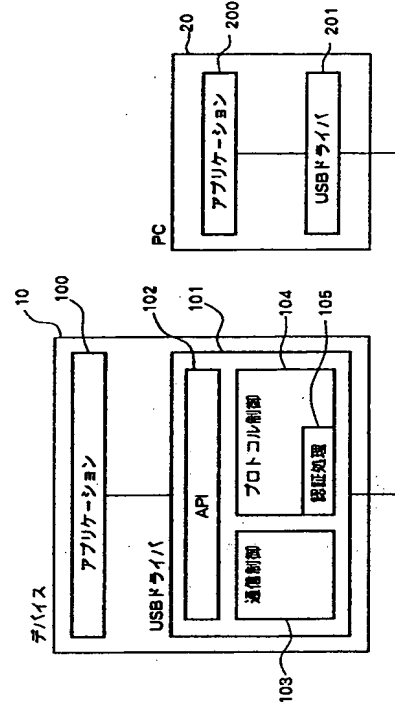
【符号の説明】

10 デバイス、101、201 ドライバ、104 プロトコル制御、105 認証処理、20 ホスト。

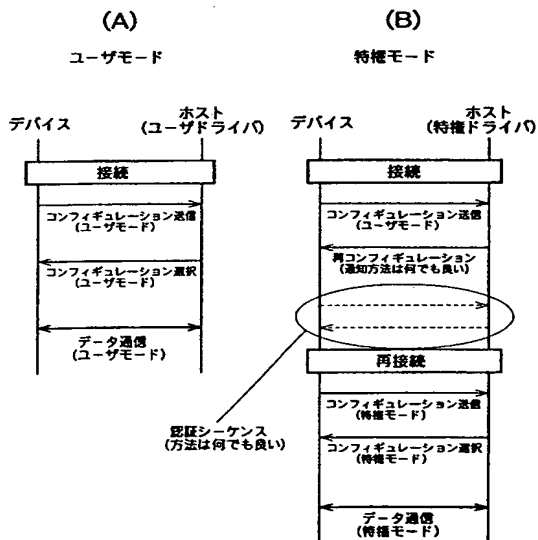
【図 1】



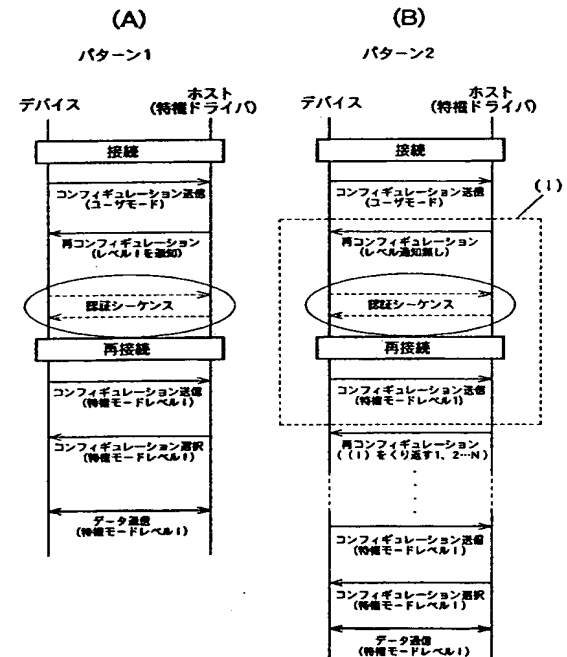
【図 2】



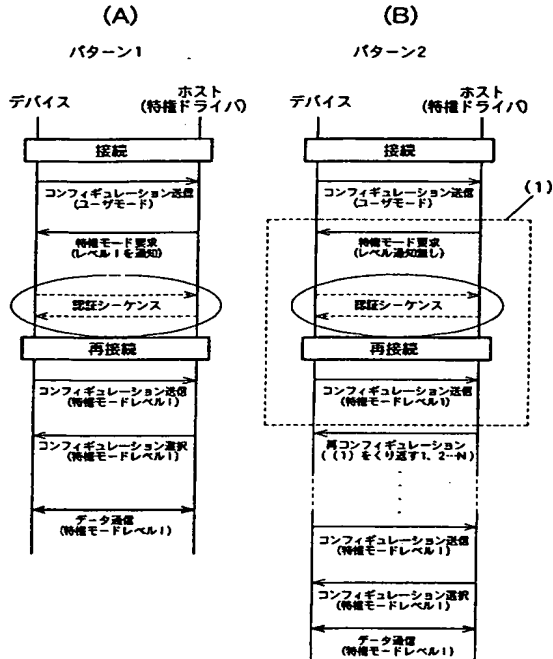
【図 3】



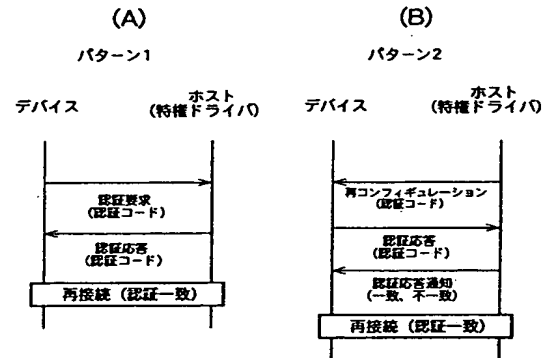
【図 4】



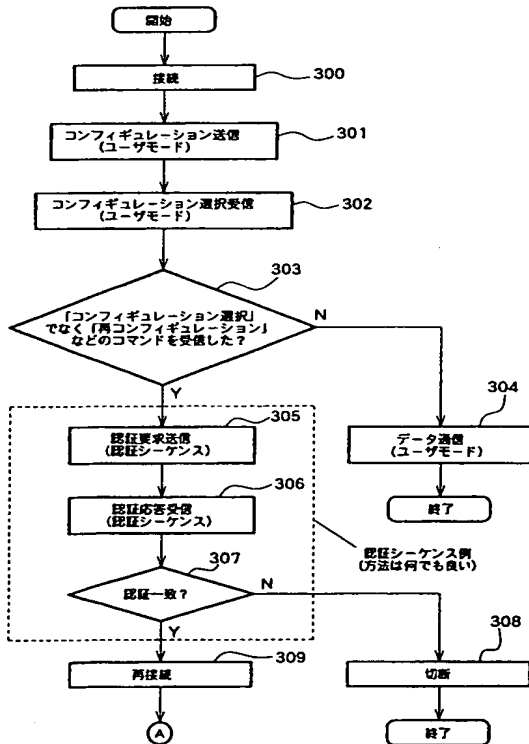
【図 5】



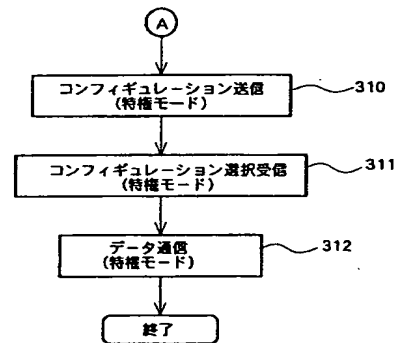
【図 6】



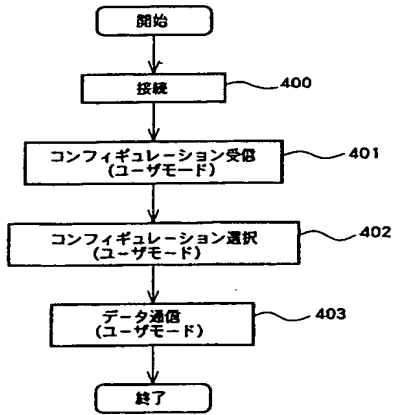
【図 7】



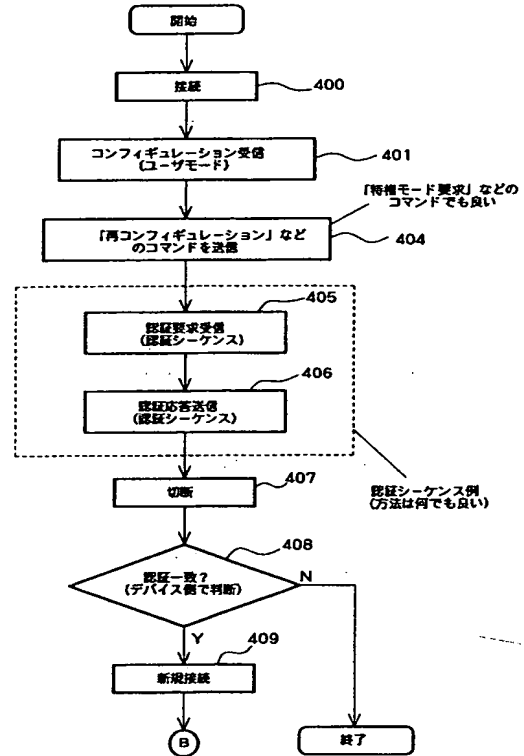
【図 8】



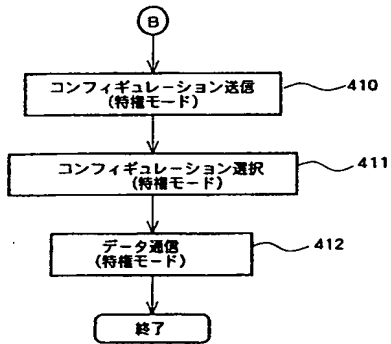
【図 9】



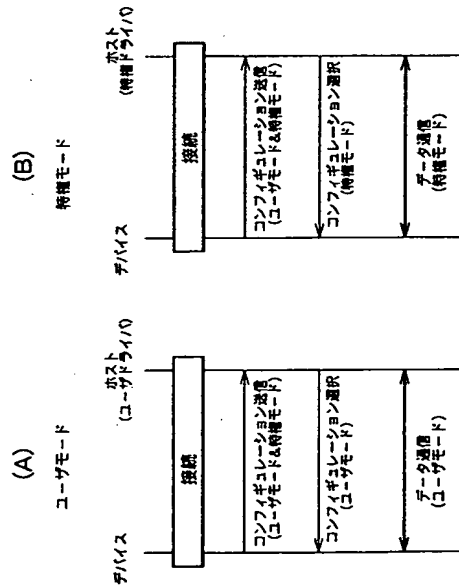
【図 10】



【図 11】



【図 12】



---

フロントページの続き

- (72)発明者 鈴木 正則  
東京都三鷹市下連雀五丁目1番1号 日本無線株式会社内
- (72)発明者 森本 真史  
東京都三鷹市下連雀五丁目1番1号 日本無線株式会社内
- (72)発明者 塩原 徹也  
東京都三鷹市下連雀五丁目1番1号 日本無線株式会社内
- Fターム(参考) 5B014 FB04 HC05  
5B077 NN02